Certificate Policies Extension

References:

ITU-T Recommendation X.509, The Directory: Authentication Framework section: 12.1
RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile
TWG-99-01, Federal PKI X.509 Certificate and CRL Extensions Profile, section: 1.2.6
MISPC, Minimum Interoperability Specification for PKI Components, Version 1, section: 3.1.3.1
DOD Medium Assurance PKI Functional Specification (DRAFT) version 0.3 (20 OCT 98), Table 13

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Certificate policies and certificate policy qualifier types may be defined by an organization. Are organizational certificate policies and certificate policy qualifier types identified by OIDs assigned according to CCITT Rec. X.660 | ISO/IEC 9834-1? [X.509: 12.2.2.6]		
Are the certificate policy qualifier types defined with the following ASN.1 object class: **CERT-POLICY-QUALIFIER ::= CLASS {** **&id OBJECT IDENTIFIER UNIQUE,** **&Qualifier OPTIONAL }** **WITH SYNTAX {** **POLICY-QUALIFIER-ID &id** **[QUALIFIER-TYPE &Qualifier] }** [X.509: 12.2.2.6]		
Does the policy qualifier type definition include: - a statement of semantics of the possible values - an indication of whether the qualifier identifier may appear in a certificate policies extension without an accompanying value and, if so, the implied semantics of such a case [X.509: 12.2.2.6]		
Can the qualifier be specified as any ASN.1 type? [X.509: 12.2.2.6]		
Can the issuer code the qualifier as an ASN.1 OCTET STRING when applications are anticipated to lack ASN.1 decoding functions? [X.509: 12.2.2.6]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Is the CA capable of issuing certificates with the Certificate Policies (CP) extension? [RFC 2459: 4.2]		
Does the issuer not include the CP extension in the Root CA certificate? [DOD: Table 12]		
Does the issuer include the CP extension in CA certificates? [TWG: 1.2.6.1]		
Does the issuer include the CP extension in EE certificates? [TWG: 1.2.6.1]		
Does the certificate contain at least one certificate policy OID? [TWG: 3.5.1, 3.5.2, 3.5.3, 3.5.4]		
Can the issuer flag the extension as critical? [X.509: 12.2.2.6]		1
Can the issuer flag the extension as non-critical? [X.509: 12.2.2.6]		1
Does the sequence of policy information terms indicate the policy that the certificate has been issued under and the purposes for which the certificate may be used? [RFC 2459: 4.2.1.5]		
Does the issuer include OID(s) for applicable certificate policy in the policyIdentifier fields? [X.509: 12.2.2.6]		
Can the issuer include policy qualifier value for a certificate policy in the policyQualifiers component? [X.509: 12.2.2.6]		
Can the issuer include policy information terms without qualifiers (i.e. consisting of only OIDs)? [X.509: 12.2.2.6, RFC 2459: 4.2.1.5]		
Does the issuer generate certificates with the policyIdentifier for the DOD Medium Assurance PKI, initially 2.16.840.1.101.2.1.11.3? [DOD: 3.2.2.1.5]		2
Can the issuer use the Certification Practice Statement (CPS) Pointer and User Notice (UN) qualifier types? [RFC 2459: 4.2.1.5]		
Does the issuer provide the CPS Pointer qualifier in the form of a URI to a CPS published by the issuer? [RFC 2459: 4.2.1.5]		
Can the issuer restrict the UN qualifier only to EE and CA certificates issued to other organizations? [RFC 2459: 4.2.1.5]		
When using the UN qualifier noticeRef field, does the issuer name an organization and identifies, by number, a particular textual statement prepared by that organization? [RFC 2459: 4.2.1.5]		
When using the UN qualifier explicitText field, does the issuer include the textual statement directly in the certificate? [RFC 2459: 4.2.1.5]		
Is the maximum size of the explicitText field is a string of 200 characters? [RFC 2459: 4.2.1.5]		
Does the issuer use VisibleString, BMPString, or UTF8String data types for the text in the noticeRef or explicitText fields? [RFC 2459: 4.2.1.5]		
In environments where multiple certificate policies apply, does the certificate issuer include certificate policy information in certificates? [X509: 12.2.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
When the CP extension is present, does the certificate user process it as a collection of OID(s)? [TWG: 1.2.6.2]		
If the extension is critical, is the certificate only used for the purpose, and according to the rules implied by one of the indicated certificate policies? [X.509: 12.2.2.6]		
If the extension is critical, is the certificate-using system able to process the qualifier value according to the rules required by a particular policy? [X.509: 12.2.2.6]		
When CP is non-critical, can the certificate user require that a particular policy be present in the extension before it will employ the certificate? [X.509: 12.2.2.6]		
When CP is non-critical, can the certificate user employ the certificate for the purposes stated by and according to the rules of the identified and qualified certificate policies? [X.509: 12.2.2.6]		
When CP is non-critical, can the certificate user employ the certificate for purposes and according to rules other then those established by the identified and qualified certificate policies? [X.509: 12.2.2.6]		
When CP is non-critical, can the certificate user employ the certificate without applying the policy qualifiers in the extension? [X.509: 12.2.2.6]		
If the certificate user has specific policy requirements, does it compare a list of those policies that they will accept against the policy OIDs in the certificate? [RFC 2459: 4.2.1.5]		
If the UN qualifier is present, does the certificate user display it to the relying party when the certificate is used? [RFC 2459: 4.2.1.5]		
Can the certificate user display all UNs in all certificates of the certification path used? [RFC 2459: 4.2.1.5]		
If duplicates of the same UN are encounter in the certification path, can the certificate user only display one copy of it? [RFC 2459: 4.2.1.5]		
Does the certificate user obtain the notice text from an originating organization?		
Can the certificate user maintain a local notice file for each organization containing the current set of notices from the organization, and extract and display the applicable notice text from it? [RFC 2459: 4.2.1.5]		
The noticeRef text may be multilingual, can the certificate user select the particular language message suitable for its own environment? [RFC 2459: 4.2.1.5]		
If a qualifier has both the noticeRef and explicitText included, and the application software can locate the notice text indicated by the noticeRef option, is that text displayed? [RFC 2459: 4.2.1.5]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
If a qualifier has both the noticeRef and explicitText included, and the application software can not locate the notice text indicated by the noticeRef option is the explicitText string displayed? [RFC 2459: 4.2.1.5]		

Other information:

1) TWG 1.2.6.1 requires setting the criticality flag. DII PKI Tables 12 and 13 has the extension as non-critical and prohibits the use of policy qualifiers.
2) At some point in the future the policy will change to: 2.16.840.1.101.2.1.11.5.

Findings:

Recommendations for Standards Work: